自动化批量部署管理的实践

摘　要：努力提高物理服务器环境下的自动化部署效率和可控管理能力，一直是运维开发人员不断追求的目标。随着新华社“媒体融合发展项目”的不断推进，在统一运维体系模式下，基础平台环境的建设在实际工作中面临着为上层业务应用系统提供基础环境支撑的任务，承担了近千台物理服务器节点的部署和运维工作，急需解决操作系统自动化批量部署和管理，及时响应业务系统部署需求的难题。

关键词：服务器；可控管理；自动化；批量
中图分类号：TP311　　文献标识码：A
文章编号：1671-0134（2017）10-119-03　　DOI：10.19483/j.cnki.11-4653/n.2017.10.050

文 / 魏海涛

1. 物理服务器部署的痛点

与传统“竖井式业务”小规模运维相比，统一运维体系下规模化的操作系统部署存在以下几方面的挑战：

（1）并存多个系统版本，数据和基础类软件要求的系统版本较低，适合容器化的应用软件要求的系统版本较高。

（2）交付界面上移，更加精细化。任务不再是简单安装操作系统，而是在统一设计要求下，完成磁盘分区和挂载、软件包安装、网络设置、NTP 时间校对、用户设置及个性化配置等。

（3）物理服务器部署节点需求数量通常在上百台，网络环境复杂，网络安全域不同，服务器具有多块网卡。

（4）部署过程中，要能够监控查看每一台服务器的详细进度。

（5）对网络连通、用户账户和软件包等进行安装结果验证。

面对以上挑战，如果靠人力部署，势必效率低下，也极易因为人为因素出现配置差错。

2. 自动化部署方案

针对操作系统规模化部署运维的弱点，我们设计了适用于新华社实际环境的操作系统自动化部署和管理方案：

（1）搭建基于 PXE 的网络自动安装环境，自定义 kickstart（简称 ks）自动安装配置文件和 shell 脚本。

（2）开发配置管理服务，以服务器设备序列号为索引，将 ks 中的配置数据抽象为参数进行封装管理，用于服务器配置管理、配置 API 查询等。

（3）开发监控服务，同样以服务器设备序列号为索引，用于监控数据上传、进度监控、安装验证等。

技术架构如图 1 所示。核心为配置管理服务和监控服务，由服务器工程师规划编制《服务器基础规划表》并上传至配置管理服务器，目标主机在自动安装时从配置管理服务器根据设备序列号加载属于自己的配置，全程进度上传监控服务器，供服务器工程师浏览验证。



图 1　系统架构

以下为各系统组件的功能描述。

DHCP 服务器，为需要安装操作系统的服务器提供 DHCP/BOOTP 服务。承担该任务的为管理网的三层交换机，安装时在交换机上的对应 VlanIf 上设置 DHCP 服务即可。相较于在服务器上配置 DHCP 服务的传统方案，在交换机上配置更为稳定，也适用于跨网段的批量服务器安装。

TFTP 服务器，对应 DHCP 服务器上的 next-server 配置，提供最小启动镜像的下载服务，承担该任务的为中控服务器。依赖操作系统的 xinetd 服务对 tftp 服务进行管理。将 CentOS 6 和 CentOS 7 等不同操作系统版本的最小启动镜像文件分开存放，实现不同操作系统的同时自动化安装。

HTTP Web 服务器，对应 TFTP 服务器上的 ks 配置文件 URL，提供 ks 配置文件以及操作系统 rpm 软件安装包的资源下载服务，承担该任务的为中控服务器。将 CentOS 6 和 CentOS 7 等不同操作系统版本的 ks 文件和 rpm 包分开存放。相较于传统方案，根据配置自动化设计，我们在这里增加了静态路由、磁盘分区等配置文件的下载。

配置管理服务器，为安装人员提供服务器配置管理操作，提供 Excel 格式的配置文件上传和浏览功能，该部分为单独开发实现，承担该任务的为中控服务器。

监控服务器，为安装人员提供服务器安装部署实时监控服务，该部分为单独开发实现，承担该任务的为中控服务器。

CMDB 服务器，服务器配置的最终状态记录数据库。

3. 自动化原理与执行流程

操作系统安装自动化的原理是基于 PXE 和 kickstart 的网络自动安装。在此基础上，我们以服务器设备序列号为索引，将个性化配置的数据抽取出来，封装为配置管理服务，结合 ks 配置文件的 pre 段和 post 段的自定义 Shell 脚本，实现个性化配置的自动化部署。

目标主机的安装执行分为两个阶段。

第一阶段为目标主机的最小安装启动镜像加载，如图 2 所示。目标主机通过支持 PXE 功能的网卡从 DHCP 服务器获取网卡 IP、网关、TFTP 服务器地址和最小安装启动镜像路径，然后从 TFTP 服务器下载启动镜像和安装启动配置文件，从配置文件中获取 ks 文件 URL 路径。pxelinux.0 为启动文件（bootfile），pxelinux.cfg/default 文件为安装启动配置文件，内含 ks 文件 URL；vmlinuz 为启动内核，initrd.img 为挂载文件系统。

第二阶段为 KickStart 方式自动安装阶段，如图 3 所示。KickStart 安装方式为我们提供了安装前（%pre）和安装后（%post）2 个自定义执行阶段，允许我们利用这 2 个阶段编写 Shell 脚本实现配置自定义。我们将相同部分直接写在 ks 文件中，包括软件安装包列表、root 及公共账号配置、SELinux 和防火墙配置、NTP 配置、DNS 配置等。对于个性化配置，编写变量 shell 脚本调用配置管理服务，利用 pre 阶段实现磁盘分区和主机名的配置导入，post 阶段实现 IP、静态路由及其他系统初始化配置。两个阶段的所有配置操作均上传监控服务器。

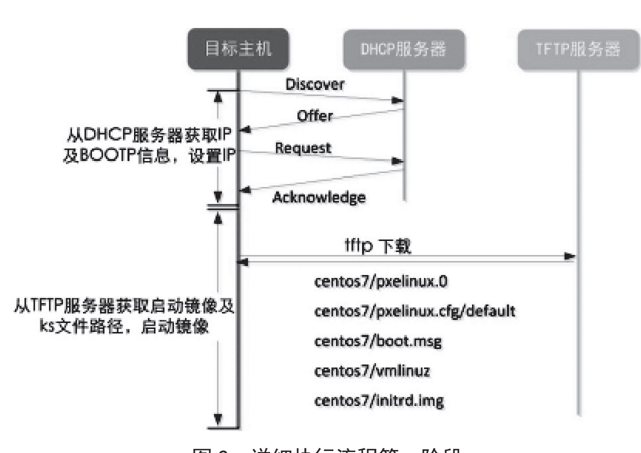


图 2　详细执行流程第一阶段



图 3　详细执行流程第二阶段

4. 配置管理和监控服务设计

配置管理和监控服务采用 nodejs 语言编写，提供配置上传和浏览、配置查询 API、安装进度监控等功能，技术架构如图 4 所示。



图 4　配置管理服务技术架构

配置管理服务具有以下几个特点：

（1）定位为工具类，采用内存数据库作为数据存储方式；配置元数据包括：服务器序列号、机柜物理位置、操作系统版本、主机名、业务网卡和带内管理网卡 IP（对应于硬件网卡位置，含 bonding）、远程带外管理卡 IP、RAID 划分、磁盘分区和挂载点，如图 5 所示。

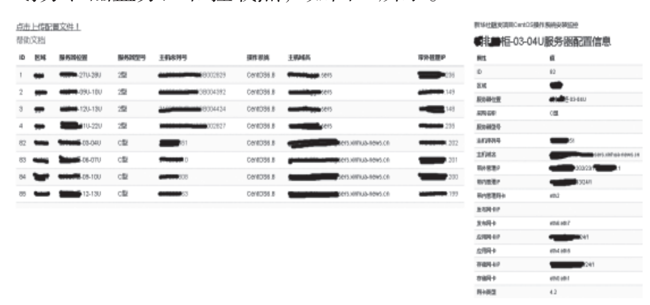


图 5　配置列表及详情页

（2）为了配合服务器工程师的工作习惯，增加了 Excel 导入配置的转换适配模块；

（3）配置查询接口采用 Restful API 格式。特别是针对网卡配置查询进行了详细设计，包括 IP 地址、网络掩码、子网、网关、网卡名称等，以应对 ks 自动安装过程中的 IP 地址类查询，减少 shell 脚本的文本解析工作。如：

http://[ip]:[port]/api/confs/[serialid]/operateIP

http://[ip]:[port]/api/confs/[serialid]/operateIPNetmask

http://[ip]:[port]/api/confs/[serialid]/operateIP

http://[ip]:[port]/api/confs/[serialid]/operateIPGateway

http://[ip]:[port]/api/confs/[serialid]/operateNic

4.1 安装实施步骤

操作系统安装自动化将服务器工程师从繁重的重复劳动中解放出来，只需少量手工操作，从而使其精力更多地集中在配置规划设计。

（1）从配置管理服务器下载《服务器基础规划表》模板，借助 Excel 表格工具对服务器配置进行规划设计。

（2）将 Excel 文档上传到配置管理服务器，同时将列表中的服务器加入到待安装服务器列表。

（3）在目标主机所在管理网当前网段的三层交换机的对应 VlanIf 上设置 DHCP 服务配置 DHCP 服务，开始安装系统。

（4）通过监控服务页面浏览安装进度（见图 6），同时可以访问每台服务器的带外管理地址，通过打开 KVM 远程 Console 来查看系统安装情况（见图 7）。

（5）安装完成后，通过安装管理界面保存此次安装过程和结果。

图 6　安装监控页面

图 7　服务器安装界面

4.2 实施中的一些经验

尽可能降低业务系统对基础环境的个性化要求，强制约束系统命名规范、用户账号规范、操作系统版本等，是实现自动化部署和提高可控管理能力的先决条件。为此，我们重点从以下两个方面对业务应用系统做出限制。

（1）制定系统部署规范，保证系统部署的一致性。我们制定了《主机域名和内部服务域名命名规范》、《用户账户和目录使用规范》、《操作系统初始化规范》、《多网卡 IP 使用规范》。

（2）强制操作系统基线版本。综合考虑基础软件兼容性、操作系统稳定性和官方维护支持期限，我们选用了 CentOS6.8 和 CentOS7.3 作为操作系统基线版本。对于数据库、大数据等数据类软件，考虑到软件本身的兼容性和稳定性，部署到 CentOS6.8，对于移植性较好的 Java/J2EE 等应用，适合容器化扩展的，部署到 CentOS7.3。CentOS 官方提供维护支持的操作系统截至日期见表 1 。

表 1　操作系统官方维护截至日期

官方提供维护支持的操作系统截至日期		
	CentOS6	CentOS7
全部更新	2017 年 5 月 10 日	2020 年四季度
维护更新	2020 年 11 月 30 日	2024 年 1 月 30 日

（翻译自：https://wiki.centos.org/About/Product）

5. 总结

该解决方案在传统的自动化部署方案基础上，根据新华社媒体融合发展项目的特点进行了优化完善，提高了服务器规模化部署的配置管理能力，增强了部署管理的可视化验证。在新华社融发项目的实践中，该方案从一定程度上解放了服务器工程师的重复繁重劳动，实现了系统批量安装自动化，极大地提高了系统部署效率，增强了系统运维管理能力，解决了系统按需按期交付的难题。媒

参考文献

[1] Kickstart documentation. http://pykickstart.readthedocs.io/en/latest/

[2] BOOTP. https://en.wikipedia.org/wiki/Bootstrap_Protocol

[3] DHCP. https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[4] DHCP RFC. https://tools.ietf.org/html/rfc2132

[5] PXE. https://en.wikipedia.org/wiki/Preboot_Execution_Environment

（作者单位：新华社技术局）